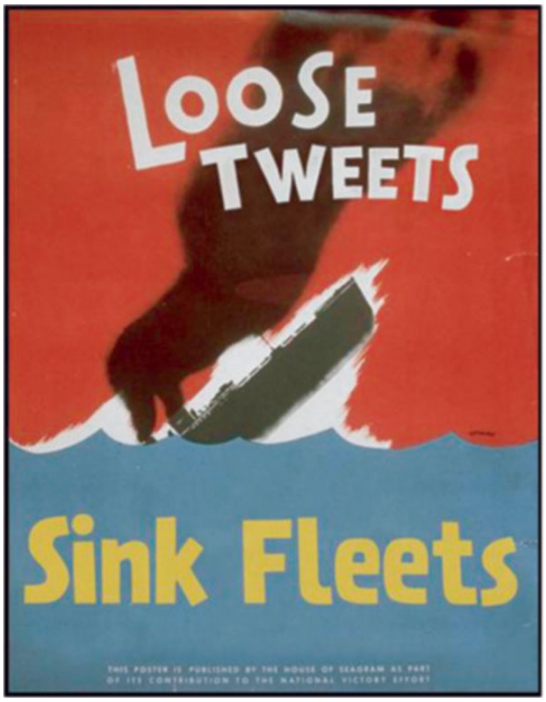
WHAT IS SOCIAL MEDIA?

Social Media, also referred to as Web 2.0, is a collection of internet-based tools that facilitate social interaction and collaboration. Whereas traditional media enables a "one-to-many" communications model, social media enables a "many-to-many" communications model. The success of social media stems from its ability to connect people to people and information through online networks, communities, dialogues, and information sharing.

Privacy and Security in Social Media - Why be careful?

With rapidly developing technology and ever-expanding user bases, it is vital that one understands the potential risks to privacy and security in social media. Threats include human or electronic Social Engineering tactics aimed at obtaining personal or sensitive information, such as:

- "**Phishing**" – tricking a user to gain information or access to a system by posing as an individual or entity the user trusts
- "**Spear Phishing**" – tricking a user to gain information by selectively targeting a recipient with a thorough understanding of the target's organization. This is commonly done in a business setting by using references or jargon specific to the organization.
- "**Pharming**" – redirecting website traffic to a false landing page that exploits the target's server software to gain information
- "**Keystroke Logging**" – software hidden in downloads which logs every key stroke giving adversaries instant access to all typed information
- "**Steganography**" – a method of concealing data in another media type, often undetectable to the human eye or ear, such as binary code in image pixels.



Additionally, seemingly innocuous activities such as sharing personal photos online with friends or having easy (yet unsecure) passwords can be a risk for identity theft or information leaks. Providing personally identifiable information (PII) via social media tools, including name, address, phone number, and daily activities, can be unsafe when in the wrong hands.

Commercial Social Media Tools outside the Government Network

The DoD is careful about leveraging commercial social media tools that exist outside of the Government Network, also known as the Non-classified Internet Protocol Router Network (NIPRNet). The most common use of these tools is to engage a broader public as part of a larger agency strategy, but users should always be aware of the information shared via these platforms. Because of the ease of use and popularity of these sites, they are often targets for Social Engineering and cyber attacks.

Automated toolkits enable an adversary to buy and maintain thousands of domains and web accounts designed to look legitimate. Social media websites are at risk of hosting malicious code resulting in man-in-the-middle attacks designed to steal the credentials of visitors. Social Engineering techniques have improved, making online traps more difficult for end users to distinguish.

The DoD's Reaction to Social Media

In 2009, the U.S. Marine Corps banned social networking websites Facebook, Twitter, and MySpace from its networks. Today the Marines have reversed that ban and the DoD includes links to social media sites on their main website. There are still concerns about the use of social media tools in the DoD, and the potential risks.

On December 8th, 2009, the White House issued the Open Government Directive requiring federal agencies to achieve transparency, participation, and collaboration. This has resulted in the increased use of common social media tools

WHAT IS SOCIAL MEDIA?

within the Federal Government, DoD and the Services. However, for protection, the directive states that:

> "...the presumption of openness precludes the legitimate protection of information whose release would threaten national security, invade personal privacy, breach confidentiality, or damage other genuinely compelling interests."

The DoD and Services are working to balance the advantages of social media while understanding the risks to privacy and national security. Draft Directive-Type Memorandum (DTM) 09-026 "Responsible and Effective Use of Internet-based Capabilities" establishes DoD policy for the use of these tools, including publicly accessible social networking services not owned by the DoD. The DoD encourages the use of Internet-based capabilities to build an information advantage for personnel and mission partners, but is careful about managing risk.

Government-sponsored Web 2.0 Tools inside the Government Network

Government-sponsored social media tools have recently emerged to promote collaboration among government and military communities, while maintaining a secure environment. All of the tools below are located inside the Government network and require a .gov or .mil email address to access and in some cases a DoD sponsor.

Intelink - www.intelink.gov
Intelink has a variety of capabilities, including a collaborative workspace with a group website that features a shared calendar and shared task lists, document libraries, and RSS feeds. In addition, Intelink has a wiki, blog, and instant messaging capability, as well as document, image, and video sharing features. It is also certified for posting Personally Identifiable Information (PII). Any person with a .gov or .mil email address can sign up online for Intelink, but may require access approval from the site administrator in order to view specific pages.

Army Knowledge Online (AKO)/Defense Knowledge Online (DKO) - www.us.army.mil
Originally developed by the Army and later adopted by the DoD, AKO/DKO provides social media capabilities such as chat features, blogs, wikis, and the MilSuite tools that support a virtual workforce by allowing users to connect with people and knowledge in real time. With an approved username and password, DoD employees can enter AKO/DKO with Common Access Card (CAC), login, and pin. AKO/DKO can be accessed from outside the government network, but government contractors and non-DoD employees require DoD-employee sponsorship to sign up for a username.

Defense Connect Online (DCO) - www.dco.dod.mil
DCO is comprised of two main collaborative capabilities: a web conferencing tool based on Adobe Connect and a chat tool. DCO can also be used to share and collaborate on documents remotely and to host video teleconferences via the internet. Access to DCO requires a CAC to register for a username and password. Once registered, DCO can be accessed via user name and password and participants without a .gov or .mil address can be invited to attend specific meetings by registered users.